Department of Homeland Security Daily Open Source Infrastructure Report for 10 December 2007

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- The Los Angeles Times reports that, according to a study by the U.S. Geological Survey released Tuesday, ash from wildfires in Southern California's residential neighborhoods poses a serious threat to people and ecosystems because it is extremely caustic and contains high levels of toxic metals. The scientists warned that rainstorms, which are forecast for the region beginning Friday, are likely to wash the dangerous substances into waterways. (See item **18**)
- According to Techworld.com and other outlets, hackers succeeded in breaking into the computer systems of two of the U.S.' most important science labs, the Oak Ridge National Laboratory in Tennessee and Los Alamos National Laboratory in New Mexico. It appears that intruders accessed a database of visitors to the Tennessee lab between 1990 and 2004, which included their social security numbers and dates of birth, though further details of the breach are being withheld pending investigation. Three thousand researchers reportedly visited the lab each year. (See item **24**)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *December 7, Bloomberg* – (National) **Nymex natural gas falls on outlook winter supplies are ample.** Natural gas in New York declined a day after a government report showed inventories are probably adequate to meet cold-weather heating needs. Stockpiles were 3.44 trillion cubic feet in the week ending November 30, the Energy Department said yesterday. The U.S. typically draws about 2 trillion cubic feet from

storage during the winter. Storage is 8.6 percent above the five-year average, according to department data. Seasonal temperatures are expected through December 20 for the largest gas consuming regions of the Northeast and Midwest, the Climate Prediction Center in Camp Springs, Maryland, said in a forecast yesterday. Normal weather patterns limit gas demand and blunt pressure for prices to rise. Utilities and other large consumers of gas store the fuel during warm-weather months to ensure adequate supplies in winter when demand outstrips production.
Source:
http://www.bloomberg.com/apps/news?pid=20601072&sid=a3b9ARIWwLdE&refer=energy

2. *December 6, KITV 4 Hawaii* – (Hawaii) **Electricity returning to Maui customers.** Maui Electric Co. was able to restore power to many customers throughout the island on Thursday following the storm that blew through the state on Wednesday. Crews worked to regain service in Kihei and Wailea after a transmission line failed at 8 a.m. In up country Maui, about 1,600 customers do not have electricity. MECO officials said crews will work through the night to repair the broken lines.
Source: http://www.msnbc.msn.com/id/22139593/

[Return to top]

Chemical Industry Sector

3. *December 6, Associated Press* – (New York) **NYC Fire code sets new hazmat rules.** New York City's first major revision to its fire code in more than 80 years requires big restaurants and department stores to have fire plans for the first time and sets rules for how to store hazardous chemicals. The 471-page draft, posted Wednesday on the fire department's Web site for public comment, was to be paired with an overhaul of the city's building code enacted earlier this year. While the building code changes drew from lessons about evacuations and fire safety learned after the September 11, 2001 attack on the World Trade Center, fire officials responded to events such as a 2003 Rhode Island nightclub fire and a 2002 Manhattan building explosion. Federal investigators of the 2002 blast, which injured dozens of people at the Kaltech Industries sign-making plant, recommended an overhaul of the code. The blast had erupted in the basement, where the company was mixing chemicals including nitric acid and lacquer thinner. The proposed changes to the code require businesses to let the fire department know where and how they are storing a long list of flammable chemicals including gasoline, diesel fuel, and chemicals used at nail salons and dry cleaners. The new code is needed to control hazardous chemicals, said the interim executive of the U.S. Chemical Safety and Hazard Investigation Board.
Source: http://biz.yahoo.com/ap/071206/ny_fire_code.html?.v=1

4. *December 5, Post Star* – (New York) **Finch Paper cited for accidental release of chemical.** The New York Department of Environmental Conservation (DEC) has cited Finch Paper LLC with two violations for a spill in early November. A valve to a 100,000-gallon tank at Finch Paper malfunctioned on November 6, sending thousands of gallons of ammonium bisulfite and organic wood matter onto the floor. The material

overflowed and roughly 1,000 gallons ended up in the Hudson River. A DEC spokesman said Wednesday that Finch Paper received notice of violations for discharging wastes into surface water and discharging waste without a permit. The waste was discharged through a storm water pipe and into the river.
Source: http://www.poststar.com/articles/2007/12/05/news/latest/doc47576146121a7701046936.txt

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *December 7, Centre Daily Times* – (Pennsylvania) **Official lauds response to reactor leak.** The U.S. Nuclear Regulatory Commission chairman praised Penn State officials on Thursday for their handling of a water leak at the Breazeale Nuclear Reactor. "From a regulatory standpoint, they did what they should do," the chairman said during a visit to Penn State. He said the university fulfilled two key requirements: swift identification of the problem and a prompt fix. "Penn State reacted appropriately." Workers at the facility realized October 9 that water was leaking from the 71,000-gallon pool that holds the reactor. The loss at one point was estimated in the range of 10 gallons an hour. Water there is "slightly radioactive" — too radioactive to meet federal drinking-water standards, but not radioactive enough to pose any kind of health hazard when it is diluted in groundwater. Penn State quickly shut down the reactor and hired a contractor to help find the problem and a fix.
Source: http://www.centredaily.com/news/local/story/282211.html

6. *December 7, Bloomberg* – (Idaho) **New nuclear plant in Idaho?** MidAmerican Energy Holdings Co. informed regulators that it intends to seek a license for a new nuclear power plant in Idaho. If the company decides to proceed with plans for a site near Boise, it would be the first commercial nuclear power plant in Idaho. MidAmerican, based in Des Moines, Iowa, could be one of two companies seeking to build a reactor in Idaho. Alternative Energy Holdings Inc. announced plans in December 2006 to build a reactor in the state. The Nuclear Regulatory Commission expects to receive applications by 2009 for as many as 32 new U.S. reactors. NRG Energy Inc., the Tennessee Valley Authority, and Dominion Resources Inc. have submitted complete applications so far.
Source: http://deseretnews.com/dn/view/0,5143,695233850,00.html

7. *December 6, Nuclear Regulatory Commission* – *(National)* **NRC orders fingerprinting and criminal history checks for access to certain radioactive materials.** The Nuclear Regulatory Commission issued an order to nearly 1,000 licensees to begin fingerprinting and criminal history checks for all persons granted unescorted access to certain radioactive materials. The order applies to NRC licensees in industry, academia, and medicine that are licensed to possess "radioactive materials in quantities of concern" from a security perspective. These quantities are essentially equivalent to Category 1 and Category 2 sources as defined in the International Atomic Energy Agency's Code of Conduct on the Safety and Security of Radioactive Sources. The order implements requirements contained in the Energy Policy Act of 2005. The agency plans to develop a

proposed rule to make the new requirements part of its regulations. The order is being issued to implement the requirement while the rule is being developed. The order, including details of how the new requirements are to be implemented, will be published soon in the Federal Register.
Source: http://www.nrc.gov/reading-rm/doc-collections/news/2007/07-163.html

[Return to top]

Defense Industrial Base Sector

8. *December 6, Business Journal of Milwaukee* – (National) **Oshkosh Truck gets $27.7 million defense order.** Oshkosh Truck Corporation has received an order from the U.S. Department of Defense to build 112 more medium tactical vehicle replacement (MTVR) trucks for the U.S. Navy under a contract valued at $27.7 million. Work is expected to be completed by September 2010, the Defense Department said Wednesday. Oshkosh Truck is the sole supplier of the MTVR family of vehicles for the U.S. military.
Source:
http://www.bizjournals.com/milwaukee/stories/2007/12/03/daily46.html?ana=from_rss

9. *December 6, United Press International* **–** (National) **GDAIS wins U.S., U.K. sub system contract.** GDAIS has won a new fire control system contract for British and U.S. ballistic missile submarines. "The U.S. Navy has awarded General Dynamics Advanced Information Systems a $91 million contract to continue providing modifications and support for fire control systems aboard U.S. and British ballistic missile submarines – SSBN – and for the attack weapons control system aboard U.S. guided missile submarines – SSGN. General Dynamics Advanced Information Systems is a business unit of General Dynamics," the company said in a statement Monday. General Dynamics said it would "provide operational support, repair, installation, checkout, development, production, and training systems for U.S. and British submarines. In addition, the contract includes development to extend the life of the Mk 6 missile guidance system. Work will be performed in Pittsfield, Massachusetts, and is expected to be completed by April 2011."
Source:
http://www.upi.com/International_Security/Industry/Briefing/2007/12/06/gdais_wins_us_uk_sub_system_contract/3903/

[Return to top]

Banking and Finance Sector

10. *December 7, WISN 12 Milwaukee* – (Wisconsin) **Better Business Bureau warns holiday shoppers of loan scam.** The Wisconsin Better Business Bureau received complaints about a loan scam from a bogus company called Plan Group Investment, which claims to be located in downtown Milwaukee. People are told they are pre-approved for a loan worth thousands of dollars, but they must first wire a fee to Canada. "It usually amounts to $2,300. We had a victim here in Wisconsin that lost $13,000," said a Better Business Bureau official. The bureau said these companies often change

names and are more active this time of year because they know people are worried about paying their holiday bills.
Source: http://www.wisn.com/consumer/14796197/detail.html

11. *December 6, Star Tribune* – (Minnesota; National) **Catholic Charities warns of scam about e-mail claiming cash award.** Catholic Charities warned Thursday that some Minnesotans have received e-mail messages falsely saying the agency has awarded them $2.5 million, which they can collect by giving personal information. The bogus e-mail says that the recipient has been given one of four annual $2.5 million awards by Catholic Charities of the Archdiocese of Rome. (There is no Catholic Charities in Europe; a similar organization there is called Caritas). The e-mails have also appeared in other states.
Source: http://www.startribune.com/local/12234076.html

[Return to top]

Transportation Sector

12. *December 7, Associated Press* – (Pennsylvania) **Pennsylvania Bridge collapses.** A 116-year-old bridge collapsed shortly after a snow plow crossed it Thursday night, prompting closure of a rural road, but causing no injuries, an official said. Details about the cause and nature of the collapse or the condition of the bridge were not immediately available, said a Pennsylvania Department of Transportation spokesman. The single-lane bridge was located along state Route 1012 between the intersections with Route 53 in Clearfield Township and First Street in Dean Township, Pennsylvania. Officials closed that section of the road to traffic and opened a 9-mile detour. PennDOT said in a statement that it will start an immediate investigation into the cause of the collapse. The bridge was built in 1891 and was used by about 270 vehicles daily.
Source:
http://ap.google.com/article/ALeqM5izJsyT6Qnq6DE5MEB6fBdW20Aw6wD8TCF95O0

13. *December 7, Express* – (District of Columbia) **Man arrested in Metro bomb scare at Pentagon.** Metrorail was shutdown at the Pentagon station Thursday afternoon in Washington, D.C., due to a bomb scare. According to Metro, a Chinese national living in Fairfax County, Virginia, allegedly claimed that another man was carrying a briefcase with a bomb in it. The station was closed at 2:42 p.m. as law enforcement officials investigated the suspicious package in question, which was located near the station faregates. In the end, nothing was identified as dangerous and the station was reopened at 4 p.m. Residual delays lasted into the early evening rush. The man, who made the initial report, was charged with making a false bomb threat and disorderly conduct, which are felonies that carry a possible 10-year prison sentence.
Source:
http://www.readexpress.com/read_freeride/2007/12/man_arrested_in_metro_bomb_scare_at_pent.php

14. *December 6, Associated Press* – (New York) **TSA screener boards plane sans ticket.**

A security screener at Kennedy International Airport in New York trying to see his parents off on a trip boarded their plane bound for the United Arab Emirates without a ticket or a boarding pass Thursday and was arrested, authorities said. When the plane's doors shut, he notified a flight attendant, said a spokesman for the Port Authority of New York and New Jersey. Port Authority police arrested the man on a misdemeanor charge of criminal trespass and released him later, said a Transportation Security Administration spokeswoman**.**
Source: http://news.yahoo.com/s/ap/20071207/ap_on_re_us/airport_breach

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture and Food Sector

15. *December 6, Associated Press* – (National) **Cattle fed distiller's grain prone to E. coli, study suggests.** In a study that could have far-reaching food safety implications, researchers at Kansas State University have found that cattle fed a byproduct of ethanol production are twice as likely to carry a potentially deadly strain of E. coli bacteria. The E. coli 0157 strain studied by Kansas State University is the same kind found in a series of recent illnesses and massive recalls of contaminated meat — although the Kansas State study itself did not link the ethanol byproducts to those specific cases. Both the researchers and meat industry representatives acknowledge that more work must be done to evaluate what the finding means in real-world conditions. The United States has about 73,000 cases of E. coli infection and 61 deaths each year, according to the Centers for Disease Control and Prevention, and most cases are caused by eating contaminated hamburger.
Source: http://www.chron.com/disp/story.mpl/ap/tx/5357475.html

[Return to top]

Water Sector

16. *December 6, Canadian Press* – (National) **Michigan legislature starts approval process for regional Great Lakes compact.** The Michigan legislature on Wednesday began passing a regional compact to prevent Great Lakes water from being sent to other regions. But final approval is not expected until January, at the earliest, because of disputes over related legislation involving large-scale water withdrawals from Michigan lakes and waterways. All eight states adjoining the Great Lakes must ratify the compact for it to take effect. It has been approved by Illinois and Minnesota. Congress also must give its approval. Environmental groups, farmers, and manufacturers oppose the legislation. The legislation would primarily affect large-scale water operations with new or expanded water use, grandfathering in existing users as long as their water use does

not rise.
Source: http://canadianpress.google.com/article/ALeqM5hInBYO0uTxHgkrof--h4bl6kg8Wg

17. *December 6, Baltimore Sun* – (Mid-Atlantic) **2010 goals for bay out of reach.** The top elected officials from the Chesapeake Bay region acknowledged yesterday that they will not achieve their goals for cleaning up the bay by 2010. High concentrations of those pollutants in the bay contribute to poor water quality and "dead zones," in which there is too little oxygen in the water to support aquatic life. Members of the Chesapeake Bay Executive Council -- which includes the governors of Maryland, Virginia and Pennsylvania, and the mayor of Washington -- said they will enact programs and policies by 2010 to reach the benchmarks for reducing pollutants such as nitrogen and phosphorus in the bay and its tributaries. To that end, the governors and Washington, D.C.'s mayor sent a letter to congressional leaders yesterday urging them to enact President Bush's farm bill, now stalled in the U.S. Senate. That legislation, if enacted, would provide $150 million to $160 million more per year to improve agricultural conservation in the Chesapeake Bay region.
Source: http://www.baltimoresun.com/news/local/bal-md.bay06dec06,0,3307793.story

18. *December 5, Los Angeles Times* – (National) **Wildfires leave caustic ash, study finds.** Ash from wildfires in Southern California's residential neighborhoods poses a serious threat to people and ecosystems because it is extremely caustic and contains high levels of arsenic, lead, and other toxic metals, according to a study by the U.S. Geological Survey released Tuesday. The scientists warned that rainstorms, which are forecast for the region beginning Friday, are likely to wash the dangerous substances into waterways, polluting streams and threatening wildlife. Some ash collected in residential areas after the October fires registered a pH of 12.7, a level more caustic than ammonia and nearly as caustic as lye. Metals, particularly arsenic, were found in such high concentrations in the ash that they would violate federal standards for cleaning up hazardous waste sites. Metals could have come from treated wood in decks, old lead-based paint, plumbing solder, and other household substances.
Source: http://www.latimes.com/news/printedition/california/la-me-ash5dec05,1,5659402.story?coll=la-headlines-pe-california

[Return to top]

Public Health and Healthcare Sector

19. *December 7, Reuters* – (International) **China says father of bird flu victim also infected.** The father of a Chinese man who died from the H5N1 strain of bird flu last week has also been diagnosed with the disease, authorities said on Friday. This latest case raises the concern that the man could have contracted the virus from his son, indicating person-to-person transmission, which would be the first step in a global pandemic. The Xinhua news agency had earlier reported that the son had had no contact with dead poultry and there had been no reported poultry outbreak in the province. The latest report did not say whether contact with infected poultry had been confirmed in either of the infections.

Source: http://www.alertnet.org/thenews/newsdesk/SP216287.htm

20. *December 7, Reuters* – (International) **Panic spreads as Uganda reports 101 Ebola cases.** Uganda has 101 suspected cases of Ebola fever and hundreds more people being closely monitored, officials said on Friday, as fear grew in Uganda and neighboring countries that the deadly virus might spread. 22 people have died so far of the fever and the minister of State for primary health-care told journalists that 11 health workers have fallen sick. Another 338 people are being monitored because they came into contact with those infected by virus. Kenya is screening Ugandans at its western border, and Rwanda said it had set up mobile clinics and isolation wards at border posts with Uganda. The four-month delay between the start of the outbreak and confirmation last week that it was Ebola has raised suspicions the government covered it up so as not to scare delegates – Britain's Queen Elizabeth and 53 heads of government -- who met in Kampala two weeks ago for a Commonwealth summit, although Uganda's government denies this.
Source: http://www.reuters.com/article/latestCrisis/idUSL07634188

21. *December 6, BBC* – (International) **Bird flu protection zone 'lifted.'** While the source of the H5N1 avian flu outbreak in Suffolk remains unknown, the protection and surveillance zones there are to be lifted. If there are no further cases, the first protection zone will be lifted on 8 December, followed by the second protection zone on 10 December. The wider surveillance and restriction zones imposed in November are due to be lifted on 19 December. Other restrictions on bird movements and gatherings will remain in place. Wild birds have not been ruled out as the cause of the outbreak.
Source: http://news.bbc.co.uk/2/hi/uk_news/7130710.stm

Government Facilities Sector

Nothing to report.

[Return to top]

Emergency Services Sector

22. *December 7, The Tribune* – (California) **County will get federal dollars for emergencies.** More than half a million dollars in Homeland Security funds will come to San Luis Obispo County, California, which will spend it on emergency vehicles, a tsunami evacuation plan, shelter for animals, and other purposes. President Bush has threatened to cut back on Homeland Security expenditures for next year, but the 2007 grants remain intact, according to the manager of the county's Office of Emergency Services. Plans for the $547,000 appropriation include, a "tactical intervention rescue vehicle, a tsunami evacuation plan, equipment to protect law enforcement officers from chemical attack, hazardous material suits, and public health and emergency medical training on vaccinations in case of disease or bioterrorism."
Source: http://www.sanluisobispo.com/news/local/story/213509.html

23. *December 6, Asbury Park Press* – (New Jersey) **Rapid Response Institute awarded contract.** Monmouth University's Rapid Response Institute has been awarded a $1 million contract from the Department of Defense to develop the first phase of an All Hazards Tool and Exercise Deployment Program. The Rapid Response Institute was initiated in 2004 with support from the New Jersey Congressional delegation, according to a news release from the university. The university's rapid response center works with the military, including Fort Monmouth and Fort Dix, to develop a coordinated communications system that will allow local, county, regional, state and federal agencies to exchange information and thus respond more effectively to biological or chemical attack, disease outbreak, or natural disaster. While the current goal is regional and statewide use, university officials have said the center ultimately would be able to exchange data worldwide, assess danger elsewhere, and decide whether that danger could affect New Jerseyans. Phase 1 will develop the specifications and requirements for an All Hazards Software Exercise Tool aimed at improving military effectiveness and National Guard preparedness, according to the release. The proposed effort addresses the development of an exercise system (that can be implemented and replicated throughout the military, National Guard, and the world) that most effectively ensures a rapid response to all hazards whether natural, man-made, the fight on terrorism or an act of war.
Source:
http://www.app.com/apps/pbcs.dll/article?AID=/20071206/NEWS01/712060302

[Return to top]

Information Technology

24. *December 7, Techworld.com* – (National) **Hackers launch major attack on U.S. military labs.** Hackers have succeeded in breaking into the computer systems of two of the U.S.' most important science labs, the Oak Ridge National Laboratory (ORNL) in Tennessee and Los Alamos National Laboratory in New Mexico. In what a spokesperson for the Oak Ridge facility described as a "sophisticated cyber attack," it appears that intruders accessed a database of visitors to the Tennessee lab between 1990 and 2004, which included their social security numbers and dates of birth. Three thousand researchers reportedly visit the lab each year, a who's who of the science establishment in the U.S. The attack was described as being conducted through several waves of phishing e-mails with malicious attachments, starting on October 29. Although not stated, these would presumably have launched Trojans if opened, designed to bypass security systems from within, which raises the likelihood that the attacks were targeted specifically at the lab. ORNL's director described the attacks in an e-mail to staff earlier this week as being a "coordinated attempt to gain access to computer networks at numerous laboratories and other institutions across the country." "Because of the sensitive nature of this event, the laboratory will be unable for some period to discuss further details until we better understand the full nature of this attack," he added. The ORNL has set up a Web page giving an official statement on the attacks, with advice to employees and visitors that they should inform credit agencies so as to minimize the possibility of identity theft. Less is known about the attacks said to have been launched

against the ORNL's sister-institution at Los Alamos, but the two are said to be linked. It has not been confirmed that the latter facility was penetrated successfully, though given that a Los Alamos spokesman said that staff had been notified of an attack on November 9 -- days after the earliest attack wave on the ORNL -- the assumption is that something untoward happened there as well, and probably at other science labs across the U.S. The ORNL is a multipurpose science lab, a site of technological expertise used in homeland security and military research, and also the site of one of the world's fastest supercomputers. Los Alamos operates a similar multi-disciplinary approach, but specializes in nuclear weapons research, one of only two such sites doing such top-secret work in the U.S.
Source: http://www.infoworld.com/article/07/12/07/Hackers-launch-attack-on-U.S.-military-labs_1.html

25. *December 7, Securitypark.co.uk* – (International) **Cyber criminals steal data from Fasthosts and force hundreds of websites to shut down.** Hundreds of websites have been shut down temporarily by one of the largest web hosting companies in Britain after the personal details of customers were stolen by computer hackers. The hackers managed to access the "master database" of Fasthosts for information, including addresses, bank details, e-mails, and passwords. The action is expected to lose vital business for hundreds of small companies in the run-up to Christmas. "The theft of data from Fasthosts is a further example of cyber criminals' continual attempts to target large organizations and businesses in order to access to vast quantities of sensitive data. Businesses are already reporting large financial losses and fear that their businesses will be forced to close as a direct result. This is not a small scale attack by any stretch of the imagination and there is potential for the thieves to have accessed everything on the database. The growing number of incidents of this type highlights the extensive value such data can provide for cyber criminals with malicious intent. Companies of all sizes need to take note and learn from these highly publicized mistakes and continue to prioritize their security procedures in order to maintain maximum data safety." commented a security analyst from McAfee.
Source:
http://www.securitypark.co.uk/security_article.asp?articleid=260173&Categoryid=1

26. *December 7, Vnunet.com* – (National) **Staff wireless networks put data at risk.** A Wi-Fi management firm has warned that companies may be unaware that their data is open to hackers because staff members have set up their own wireless networks. AirMagnet claimed that one employee could put the whole network at risk simply by plugging their own router into an access point. "We go into a lot of companies which say 'we haven't got any wireless access' and we do a demo and three or four access points pop up," a managing director at AirMagnet said. The culprit is not necessarily attempting to breach the network, but simply wants to be able to use Wi-Fi on their laptop. "It is not always malicious but it gives you visibility," he said. AirMagnet's Air Enterprise software has a triangulation function to pinpoint the offending Wi-Fi, and can root out problems on existing wireless networks by looking for anomalies. "For example, if you normally use Netgear kit and you see a Linksys router you know that's not right," he said. "If a wireless connection is popping up at four in the morning for an hour that's definitely

malicious but it won't be picked up if no-one is monitoring it." He also poured scorn on companies which believe they are protected because they are using the Wired Equivalent Privacy security algorithm. "Everyone knows that Wep is untrustworthy and can be easily cracked," he said.
Source: http://www.vnunet.com/vnunet/news/2205251/employee-wireless-networks-put

27. *December 6, Computerweekly.com* – (International) **Businesses at risk from hacker attacks, warns Finjan.** Businesses around the world are at risk from attacks distributed in China and existing signature-based anti-virus software and URL-based web monitoring may not be enough to protect end-users, researchers have warned. A study from Finjan, a supplier of secure web gateway products, has reported that users' PCs are being infected by Trojans distributed from China. The company's Malicious Code Research Center (MCRC) has detected malicious activity by groups that distribute their content using a network of websites to bypass traditional information security technology. The researchers uncovered a sophisticated attack that used zero-day exploits (malware for which there is no security patch) as well as other new hacking techniques. They also discovered a centralized group of activity based from China. One of the websites in the group belongs to a Chinese governmental office. The research found that these infected PCs are stealing data from organizations. Once the user's PC has been infected, the Trojan starts to send data to other websites in the network, which are hard to detect. Additional sites in the network monitor and control the attack using statistics about how many users visit the site and how many got infected. The Trojans also collect data from the user, including which operating system is used, the applications that are running, users' personal information, and what security systems are installed. The information collected by the Trojan network is then fed into other sites, which refine the attack. Signature-based antivirus software is unable to protect users against this attack, Finjan's chief technology officer said. "In order to have a signature for your anti-virus software, a researcher needs to create a signature. But each time it is downloaded a new version of the Trojan is created." IT directors will also be unable to block access to malicious website, he warned. "The website URLs are being changed dynamically so you will never be able to keep your website monitoring database up to date. Hackers will change the location of the malicious code."
Source: http://www.computerweekly.com/Articles/2007/12/06/228514/businesses-at-risk-from-hacker-attacks-warns-finjan.htm

28. *December 5, Eweek.com* – (National) **Attackers exploiting QuickTime RTSP flaw in the wild.** The unsavory types have done exactly as security researchers warned they would, releasing into the wild exploit code for a vulnerability in how Apple's QuickTime Player 7.3 handles RTSP (Real Time Streaming Protocol) responses from a video/audio streaming server. Symantec on December 1 spotted an attack that uses iFrame code to force a browser to send out a request to a URL embedded in an adult content site. Users visiting the site are redirected to a malicious page serving the exploit. The attacks have since then taken on new twists: attackers are now exploiting the issue through the Second Life Viewer to steal virtual money—known as Linden Dollars—from victims, Symantec's Deep Sight Alert Services said in a December 4 update to its original advisory. The mention of a virtual reality game might make the vulnerability

sound too consumer-ish for businesses to take seriously. However, with no patch available and no word from Apple on a patch ETA, there are only workarounds such as these from US-CERT (United States Computer Emergency Readiness Team), each of which "makes the use of valid QuickTime content next to impossible," the SANS Institute noted in a December 2 advisory. Anti-virus programs are picking up the exploits, but Symantec is warning people to still be careful when browsing the Web. They are also recommending that, in the absence of a patch, users run browsers at the highest security settings possible; disable QuickTime as a registered RTSP protocol handler; and filter outgoing activity over common RTSP ports, including TCP port 554 and UDP ports 6970-6999.
Source: http://www.eweek.com/article2/0,1895,2228559,00.asp

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

Nothing to report.

[Return to top]

Commercial Facilities Sector

29. *December 7, Associated Press* – (Florida) **Construction barred on former bomb range.** Officials in Orlando, Florida, suspended all building permits in the three communities after a handful of live bombs and other munitions debris were found in those areas in the past several months. The communities were built on the Army's old Pinecastle Jeep Range. Construction can resume only after the property is examined and declared bomb-free by a licensed munitions company. The U.S. Army Corps of Engineers is responsible for cleaning up the property
Source: http://www.firstcoastnews.com/news/florida/news-article.aspx?storyid=97389 .

30. *December 6, Associated Press* – (Pennsylvania) **Bank robbers leave behind fake bomb, causing evacuations.** Dauphin County, Pennsylvania, authorities say two bank robbers caused a scare by leaving behind a bag that they said contained a bomb, but actually only contained cardboard and bricks. The bank and nearby businesses were evacuated for several hours. A bomb squad removed the bag from the bank, then blasted the bag and found it never had any explosives in it
Source: http://www.pennlive.com/newsflash/pa/index.ssf?/base/news-57/11969735836740.xml&storylist=penn

[Return to top]

National Monuments & Icons Sector

Nothing to report.

[Return to top]

Dams Sector

31. *December 7, News Democrat and Leader* – (Kentucky) **Spa Lake closed, dam getting repairs.** Preparations are being made to repair Spa Lake Dam in Kentucky. The dam's integrity is in danger because of a leak and erosion caused by a sinkhole in the lake near the face of the dam. In September, the state allocated $100,000 in funding to the city of Russellville to help repair the lake's dam. Spa is a watershed lake built in 1975 for watershed protection, flood control, and water supply. The lake is about three miles long, 26.5 feet deep at the suction point, covers 240 acres and holds over one billion gallons of water under normal conditions. Currently, the lake has been intentionally drained 13.8 feet to prepare for the repairs.
Source: http://www.newsdemocratleader.com/articles/2007/12/07/news/news05.txt

32. *December 6, Chronicle* – (Washington) **Skookumchuck Dam secure, despite rumors.** A local paper received several calls Wednesday from people fearing that the earthen Skookumchuck Dam northeast of Centralia, Washington, was bursting. Fortunately, the dam is fine. "It's solid. There's no concern of it breaching," said the senior communications advisor for TransAlta USA, which bought the 1970s-era dam several years ago. The Skookumchuck Dam, which forms an eight-mile-long lake northeast of Centralia to hold water for use in the Centralia Steam-Electric plant's summer electrical power generation, was 20 feet below capacity late last week. Although it was not built as a flood control dam and can not really be operated as one, it just happens that during this flood event, the dam had plenty of capacity to hold water rushing downstream from the hills above it, the advisor said.
Source:
http://www.chronline.com/story.php?subaction=showfull&id=1196971947&archive=&start_from=&ucat=1

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389
Subscription and Distribution Information:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer